

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Bruce L. Davis

Application No.: 10/086,180

Filed: February 25, 2002

For: **DISTRIBUTION AND USE OF  
TRUSTED PHOTOS**

Examiner: S. Qureshi

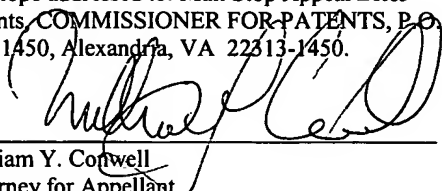
Date: November 3, 2005

Art Unit 2155

Confirmation No. 1232

**CERTIFICATE OF MAILING**

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being deposited with the United States Postal Service on November 3, 2005 as First Class Mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, VA 22313-1450.

  
William Y. Cornwell  
Attorney for Appellant

**APPEAL BRIEF**

Mail Stop: Appeal Brief – Patents  
COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This brief is in furtherance of the Notice of Appeal filed August 4, 2005. Please charge the fee required under 37 CFR 1.17(f), and any required extension of time, to deposit account 50-3284 (see transmittal letter).

I. REAL PARTY IN INTEREST.....	3
II. RELATED APPEALS AND INTERFERENCES.....	3
III. STATUS OF CLAIMS .....	3
IV. STATUS OF AMENDMENTS .....	3
V. BACKGROUND AND SUMMARY OF CLAIMED SUBJECT MATTER.....	3
VI. GROUNDS OF REJECTION.....	7
VII. ARGUMENT.....	8
1. Discussion of Rhoads 5,841,886.....	8
2. Claim 16 (§102 Rhoads) .....	8
3. Claim 17 (§ 102 Rhoads).....	10
4. Claim 18 (§ 102 Rhoads).....	10
5. Claim 19 (§ 102 Rhoads).....	11
6. Claim 20 (§ 102 Rhoads).....	12
7. Claim 1 (§ 103 Rhoads).....	12
8. Claim 2 (§ 103 Rhoads).....	13
9. Claim 3 (§ 103 Rhoads).....	14
10. Claim 4 (§ 103 Rhoads).....	14
11. Claim 5 (§ 103 Rhoads).....	14
12. Claim 6 (§ 103 Rhoads).....	15
13. Claim 7 (§ 103 Rhoads).....	15
14. Claim 8 (§ 103 Rhoads).....	15
15. Claim 9 (§ 103 Rhoads).....	16
16. Claim 10 (§ 103 Rhoads).....	16
17. Claim 11 (§ 103 Rhoads).....	16
18. Claim 12 (§ 103 Rhoads).....	17
19. Claim 13 (§ 103 Rhoads).....	17
20. Claim 14 (§ 103 Rhoads).....	17
21. Claim 15 (§ 103 Rhoads).....	17
22. Claim 21 (§ 103 Rhoads).....	18
23. Claim 22 (§ 103 Rhoads).....	18
24. Claim 23 (§ 103 Rhoads).....	19
25. Claim 24 (§ 103 Rhoads).....	19
26. Claim 25 (§ 103 Rhoads).....	20
27. Claim 26 (§ 103 Rhoads).....	20
VIII. CONCLUSION.....	21

**I. REAL PARTY IN INTEREST**

The real party in interest is Digimarc Corporation, by an assignment from the inventors recorded at Reel 12979, Frames 813-814.

**II. RELATED APPEALS AND INTERFERENCES**

None.

**III. STATUS OF CLAIMS**

Claims 1-26 stand finally rejected and are appealed.

**IV. STATUS OF AMENDMENTS**

All prior amendments have been entered.

In preparing this Brief, the undersigned noted a problem with claim 22; it depended from itself rather than claim 21 as intended. Likewise, claim 25 depended from claim 21, instead of claim 24 as intended.

An amendment submitted herewith corrects these errors. (The claims as presented in the Appendix to this Brief show claims 22 and 25 after correction.)

**V. BACKGROUND AND SUMMARY OF CLAIMED SUBJECT MATTER**

The creation of identification documents, such as identification badges, has typically required that the individual being depicted sit for a picture. This is often an inconvenience, and may result in many different photos of an individual being taken for identification documents.<sup>1</sup>

---

<sup>1</sup> Specification, page 1, lines 12-14.

Consider a different arrangement, as illustrated by the following scenario:

*An employment candidate will be interviewing at a new employer and needs an access badge.*

*The employer e-mails or otherwise sends the candidate an access code. The code is valid only for a certain time period on a given date (e.g., 9:00 a.m. – 11:00 a.m. on June 28, 1999).*

*Upon receiving the access code, the candidate downloads from the web site of the state Department of Motor Vehicles the latest copy of her driver's license photo. The DMV has already encoded this photo with hidden watermark data, which points to a corresponding database record in a state-run server. (If that server is queried with data decoded from the photograph, the server accesses the database and may reply to the inquiring computer e.g., with a text string indicating the name of the person depicted by the photograph.)*

*The employment candidate incorporates the photo obtained from the DMV into an access badge. Using a software application on her home computer (which may be provided especially for such purposes, e.g., as part of an office productivity suite), the photo is dragged into an access badge template. The access code emailed from the employer is also provided to this application. On selecting "Print," an ink-jet printer associated with the candidate's computer prints out an access badge that includes her DMV photo and her name, and is also digitally watermarked in accordance with the employer-provided access code.*

*The name printed on the badge is obtained (by the candidate's computer) from the DMV's server, in response to watermark data extracted from the photograph.*

*On the appointed day the candidate presents herself at the employer's building. At the exterior door lock, the candidate presents the home-printed badge to an optical sensor device, which reads the embedded building access code, checks it for authenticity and, if the candidate arrived within the permitted hours, unlocks the door.*

*Inside the building the candidate may encounter a security guard. Seeing an unfamiliar person, the guard may visually compare the photo on the badge with the candidate's face. Additionally, the guard can present the badge to a portable watermark reader device. The reader device decodes the watermark data from the card (e.g., from the DMV photograph), interrogates the DMV's server with this data, and receives in reply the name of the person depicted in the photograph.*

*The guard checks the name returned from the DMV server with the name printed on the badge. On seeing that the printed and DMV-indicated names match, the security guard can let the candidate pass.*

*It will be recognized that the just-described arrangement offers very high security, yet this security is achieved with without the candidate ever previously visiting the employer, without the employer knowing what the candidate looks like, and by use of an access badge produced by the candidate herself.<sup>2</sup>*

In accordance with one illustrative embodiment of the present invention, a trusted repository of images - such as an image archive maintained by a state motor vehicle licensing agency - is used to provide images for non-driver license applications. As needed, a user may electronically contact such an agency and solicit a copy of their driver license photo. The agency responds by sending an electronic version of the photo, which then can be incorporated, e.g., into an identification badge. Since the photograph comes from a trusted, independent source, it can be used in identification documents without requiring the individual to sit for another photo.<sup>3</sup>

In one particular arrangement, an individual user electronically contacts a governmental agency (such as a motor vehicle licensing agency), and solicits an image depicting the user. This image is stored in an archive maintained by the governmental agency. In response, the user electronically receives back the solicited image from the agency, and then prints a document (e.g., a photo identification document, such as a badge) incorporating the image.<sup>4</sup>

---

<sup>2</sup> Specification, page 13, line 25 – page 15, line 4.

<sup>3</sup> Specification, page 1, lines 15-21.

<sup>4</sup> See, e.g., original claim 1 (specification, page 46); specification page 13, line 31 – page 14, line 3.

The image provided by the government agency may have been processed with an identification code prior to provision to the user.<sup>5</sup> For example, the image may have been digitally watermarked with a plural-bit code that serves to identify the depicted individual.<sup>6</sup> (Such identification can be direct, or the code can comprise an index into a data structure<sup>7</sup> in which the individual user's name is stored.)

(Digital watermarking, sometimes termed "steganography," is the science of hiding secret information – often in some other data, and without leaving any apparent evidence of data alteration.<sup>8</sup> Digital watermarking can take many forms - several are detailed in patent documents incorporated-by-reference in the present specification.<sup>9</sup> One form of digital watermarking favored by the present Appellants involves making subtle changes to the luminance of pixels comprising a photograph to thereby encode a hidden multi-bit digital data payload. The changes are too slight to be perceptible to human viewers of the photo. But when such watermark-encoded printed photograph is sensed by an image sensor and computer analyzed, the encoded digital data can be recovered.)

In a second particular arrangement, the invention is a method of distributing a trusted image. A governmental agency receives an electronic request for an archived personal image from an individual depicted in said image. The image is then electronically transmitted to that individual.<sup>10</sup>

Again, the image may be processed with an identification code (e.g., by digital watermarking) prior to transmission to the individual.<sup>11</sup>

In a third particular arrangement, the invention is a document printing method. A digital photo – having plural-bit data steganographically encoded therein – is received (e.g., from an archive of facial images, such as may be maintained by a government agency). By reference to

---

<sup>5</sup> See, e.g., specification, page 13, lines 32-33.

<sup>6</sup> See, e.g., original claims 7, 8 (specification, page 46).

<sup>7</sup> See, e.g., specification, page 12, lines 4-6.

<sup>8</sup> Digital watermarking is a well developed art that is not belabored in the present specification. Instead, the present specification incorporates-by-reference earlier patents and applications on the subject. See, e.g., specification at page 7, lines 22-25; page 41, lines 26-33 (both subsequently amended by Amendment filed November 3, 2004), and incorporation-by-reference language at page 45, lines 1-2.

<sup>9</sup> *Ibid.*

<sup>10</sup> See, e.g., original claim 11 (specification at page 47); page 13, lines 31-32.

<sup>11</sup> See, e.g., specification, page 13, lines 32-33.

this steganographically encoded data, text is generated to be printed with the photo. A document (e.g., a photo identification document) is then printed, including both the text and the photo.<sup>12</sup>

The text may be generated by transmitting at least a part of the plural-bit data to a remote computer, and receiving the text back from such computer.<sup>13</sup>

In a fourth particular arrangement, the invention is a method of providing an access credential for a person – using a computer device for which that person is the proprietor (e.g., printed-at-the-person's-home).<sup>14</sup> At the computer device certain code data is received from an authority. This code data has a future time or date associated therewith.<sup>15</sup> The code data is steganographically encoded in a graphic (e.g., by the person's computer), and the encoded graphic is then presented as an access credential so as to gain access to a restricted area.<sup>16</sup>

The future time or date may specify the time/date of an event (e.g., a movie), to which the encoded graphic authorizes entry.<sup>17</sup> The encoded graphic may be printed using a printer, for which the person is also the proprietor.<sup>18</sup>

As in the earlier arrangements, the graphic may be a portrait of the person, received from a governmental agency.<sup>19</sup>

## VI. GROUND'S OF REJECTION

Claims 16-20 stand rejected under § 102 over Rhoads (5,841,886).

Claims 1-15 and 21-26 stand rejected under § 103, over the same art.

---

<sup>12</sup> See, e.g., original claim 16 (specification at page 47); page 13, line 31 – page 14, line 10.

<sup>13</sup> See, e.g., original claim 17 (specification at page 47); page 14, lines 9-10.

<sup>14</sup> See, e.g., specification, page 13, line 28 – page 14, line 20.

<sup>15</sup> *Ibid.*

<sup>16</sup> *Ibid.*

<sup>17</sup> See, e.g., specification, page 15, lines 5-10.

<sup>18</sup> See, e.g., specification, page 14, lines 6-8.

<sup>19</sup> See, e.g., specification, page 13, lines 31-32.

## VII. ARGUMENT

### 1. Discussion of Rhoads 5,841,886

In one passage cited in the Action (col. 7), Rhoads discloses that an ID document can be steganographically encoded with additional data, *e.g.*, permitting it to be validated.

For example, the photo portrait that is printed in a passport may be steganographically encoded with information that is also textually printed on the passport – such as the person’s name. To check for passport tampering, the document is scanned, and this additional information is decoded from the scan data. The name as printed on the passport is then compared with information determined from the scan data. If they do not match, then either the printed text, or the photo portrait, has been altered.

In another passage cited in the Action (*e.g.*, cols. 2-3), Rhoads teaches a personal cash card (*e.g.*, an ATM-like card) that includes a person’s photo, and also conveys a large amount of information unique to that card (*e.g.*, by watermark encoding, which may take the form of a snow-like pattern). This unique information acts like a library of one-time keys (“transaction tokens”<sup>20</sup>), which can be employed by retail store terminals to complete secure financial transactions.

### 2. Claim 16 (§102 Rhoads)

Claim 16 encompasses the arrangement noted above wherein hidden data is decoded from a photo, and, by reference to such data (*e.g.*, by querying a database with it), text is generated (*e.g.*, the database returns text specifying the name of the person in the photo). A document is then printed having both the photo and the text.

Claim 16 reads as follows:

*16. A document printing method, comprising:  
receiving a digital photo, the photo having plural-bit data steganographically*

---

<sup>20</sup> Rhoads, 5,841,886, col. 3, line 28.



*encoded therein;  
by reference to said steganographically encoded data, generating text to be  
printed with said photo; and  
printing a document including both said photo and said text.*

Rhoads does not teach the claimed method.

For example, Rhoads does not teach “by reference to said steganographically encoded data, generating text to be printed with said photo.”

Although the Action cites passages from both Rhoads’ ID document and cash card embodiments against this limitation, neither does what the claim language says.

In the ID document case, Rhoads explains that an operator may scan a passport at a visa control point to extract the steganographically-encoded information found in the passport photo (col. 7, lines 44-46). This data is then used, *e.g.*, to verify that the passport has not been altered.

While this may be regarded as “generating text” from the steganographically encoded data, there is no disclosure of then using such text to print a document. (The printed document is the *starting* point - the document from which the operator scanned the photo in which data was steganographically encoded. There is no generation of text to be printed in a text/photo document – generated by reference to the encoded data.)

In the cited passage relating to the cash card embodiment (col. 3, lines 1-7), the unique information (*e.g.*, the library of one-time transaction tokens, steganographically encoded as a snow-like pattern) is combined with the photo and printed to form a card. Again, however, it is not used in connection with generating text to be printed with the photo.

Rhoads also does not teach the concluding limitation of claim 1 - printing a document including both said photo and said [generated] text. (Col. 3, lines 1-7 is again cited for this element, but that passage discloses combining a photo with the additional data (*e.g.*, the library of one-time transaction tokens, steganographically encoded as a snow-like pattern), and printing a card from it.)

Reversal is required.

3. **Claim 17 (§ 102 Rhoads)**

Claim 17 depends from claim 16 and is similarly allowable. Moreover, claim 17 is patentable independently. The claim reads:

*17. The method of claim 16 that includes electronically transmitting at least a part of said plural-bit data to a remote computer, and receiving the text from said computer.*

The Action cites col. 2, line 64 – col. 3, line 7 for this claim limitation. However, that passage does not teach this limitation. It states:

*FIG. 1 illustrates the basic unforgeable plastic card which is quite unique to each and every user. A digital image 940 is taken of the user of the card. A computer, which is hooked into the central accounting network, 980, depicted in FIG. 5, receives the digital image 940, and after processing it (as will be described surrounding, FIG. 3) produces a final rendered image which is then printed out onto the personal cash card 950.*

This passage relates to combining a photo with steganographically encoded additional information (e.g., the library of transaction tokens, steganographically encoded as a snow-like pattern). No transmission of such data to a remote computer, and receipt of text to be printed, is taught.

Again, reversal is required.

4. **Claim 18 (§ 102 Rhoads)**

Claim 18 depends from claim 16 and is similarly allowable. Moreover, claim 18 is patentable independently. The claim reads:

*18. The method of claim 16, that includes receiving said digital photo from an archive of facial images.*

The Action states “Rhoads teaches the method of claim 16, that includes receiving the digital photo from an archive of facial images (column 3, lines 19-22).”<sup>21</sup> Not so. The cited passage reads:

*In any event, the unique information within the image on the personal cash card 950 is stored along with the basic account information in a central accounting network, 980, FIG. 5.*

The limitation of claim 18 is not taught.

Again, reversal is required.

**5. Claim 19 (§ 102 Rhoads)**

Claim 19 depends from claim 16 and is similarly allowable. Moreover, claim 19 is patentable independently. The claim reads:

*19. The method of claim 16 that includes receiving said digital photo from an image archive maintained by a government agency.*

Again, the Final Action contends that Rhoads teaches such limitation, citing two passages. Those passages read as follows:

*FIG. 1 illustrates the basic unforgeable plastic card which is quite unique to each and every user. A digital image 940 is taken of the user of the card. A computer, which is hooked into the central accounting network, 980, depicted in FIG. 5, receives the digital image 940, and after processing it (as will be described surrounding, FIG. 3) produces a final rendered image which is then printed out onto the personal cash card 950.*

and

*In this regard, reference is made to FIG. 6, which depicts a photo-ID card or document 1000 which may be, for example, a passport or visa, driver's license, credit card, government employee identification, or a private industry identification badge. For*

---

<sup>21</sup> Final Action, page 4, lines 13-14.

*convenience, such photograph-based identification documents will be collectively referred to as photo ID documents.*

It will be recognized that there is no teaching of receiving a steganographically-encoded digital photo from an image archive maintained by a government agency, so that same can be printed on a document, as required by claim 19.

Again, reversal is required.

6. **Claim 20 (§ 102 Rhoads)**

The Rhoads-based rejection of claim 20 stands or falls with the Rhoads-based rejection of claim 16.

7. **Claim 1 (§ 103 Rhoads)**

Claim 1 is an independent claim that reads as follows:

*1. A method of printing a trusted image, comprising:  
an individual user electronically contacting a governmental agency, soliciting an image depicting the user stored in an archive maintained by said governmental agency;  
electronically receiving said image from said contacted governmental agency;  
and  
printing a document incorporating said image.*

The Action wrongly asserts that Rhoads teaches an individual user “soliciting an image depicting the user stored in an archive maintained by a central network,” citing col. 3, lines 19-22.

The cited passage does not so teach. That passage reads:

*In any event, the unique information within the image on the personal cash card 950 is stored along with the basic account information in a central accounting network, 980, FIG. 5.*

Thus, the Office failed to meet its *prima facie* burden.

The Action acknowledges that Rhoads doesn't teach that the image is received by the user soliciting the image, but dismisses this as obvious – contending an artisan would have been motivated in this direction “so that the user may print an identification card.”<sup>22</sup>

However, it will be recognized that the art is silent about a user printing his or her own identification card. Indeed, it is evident that self-printing of identification cards would be *non-obvious* to an artisan, due to the obvious security shortcomings associated with such a practice.

Thus, the rejection also fails for want of a compelling rationale showing why an artisan would have modified the art to yield the claimed arrangement.

Still further, the claim requires soliciting an image from an archive maintained by a governmental agency. The Action admits Rhoads does not teach this limitation, but asserts that, because an ID card may be used for government use, it would have been obvious that the central network can be a government agency.

That's hindsight. Although government agencies have maintained image archives for years (two photos must be submitted to the U.S. State Department to obtain a passport; the passport contains only one), Appellants' specification is believed to be the first to teach or suggest that an individual may obtain their own archived photo *from* a government agency, e.g., for printing at home.

The rejection is multiply flawed and should be reversed.

**8. Claim 2 (§ 103 Rhoads)**

Claim 2 depends from claim 1 and is similarly allowable. Moreover, claim 2 is patentable independently. The claim reads:

*2. The method of claim 1 in which it is the individual user who receives said image and prints said document.*

Rhoads does not suggest such limitation. The excerpt cited in the Final Rejection in support of the rejection (col. 6, lines 50-57) does not suggest it. That passage states:

---

<sup>22</sup> Final Action, page 5, lines 18-20.

*In this regard, reference is made to FIG. 6, which depicts a photo-ID card or document 1000 which may be, for example, a passport or visa, driver's license, credit card, government employee identification, or a private industry identification badge. For convenience, such photograph-based identification documents will be collectively referred to as photo ID documents.*

It will be recognized that there is no suggestion here of an individual user receiving their own image from an archive maintained by a governmental agency, and printing their own photo document from it.

Again, the rejection should be reversed.

**9. Claim 3 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 3 stands or falls with the Rhoads-based rejection of claim 1.

**10. Claim 4 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 4 stands or falls with the Rhoads-based rejection of claim 1.

**11. Claim 5 (§ 103 Rhoads)**

Claim 5 depends from claim 1 and is similarly allowable. Moreover, claim 5 is patentable independently. The claim reads:

*5. The method of claim 1 in which the governmental agency is a motor vehicle licensing agency, and the image is a driver license photo.*

The Final Action wrongly states, “*Rhoads teaches the method of claim 1 in which the governmental agency is a motor vehicle licensing agency,*”<sup>23</sup> citing col. 6, lines 50-57. Again, Rhoads does not so teach. The cited passage reads:

*In this regard, reference is made to FIG. 6, which depicts a photo-ID card or document 1000 which may be, for example, a passport or visa, driver's license, credit card, government employee identification, or a private industry identification badge. For convenience, such photograph-based identification documents will be collectively referred to as photo ID documents.*

This does not teach soliciting an image from an archive maintained by a motor vehicle licensing agency, as required by the claim.

Again, the Office’s *prima facie* burden under § 103 has not been met. Reversal is required.

**12. Claim 6 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 6 stands or falls with the Rhoads-based rejection of claim 1.

**13. Claim 7 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 7 stands or falls with the Rhoads-based rejection of claim 1.

**14. Claim 8 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 8 stands or falls with the Rhoads-based rejection of claim 7.

---

<sup>23</sup> Final Action, page 6, lines 5-6.

**15. Claim 9 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 9 stands or falls with the Rhoads-based rejection of claim 8.

**16. Claim 10 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 10 stands or falls with the Rhoads-based rejection of claim 1.

**17. Claim 11 (§ 103 Rhoads)**

Claim 11 is an independent claim that reads as follows:

*11. A method of distributing a trusted image, comprising:  
at a governmental agency, receiving an electronic request for an archived  
personal image from an individual depicted in said image; and  
electronically transmitting said image to said individual.*

Again, the Final Rejection wrongly cites Rhoads at col. 2, line 64 – col. 3, line 4, as teaching the first claim limitation (except the “governmental agency”).<sup>24</sup> It does not. That passage states:

*FIG. 1 illustrates the basic unforgeable plastic card which is quite unique to each and every user. A digital image 940 is taken of the user of the card. A computer, which is hooked into the central accounting network, 980, depicted in FIG. 5, receives the digital image 940, and after processing it (as will be described surrounding, FIG. 3) produces a final rendered image which is then printed out onto the personal cash card 950.*

Nothing here teaches “receiving an electronic request for an archived personal image from an individual depicted in the image.”

---

<sup>24</sup> Final Action, page 7, lines 1-2.



Again, the rejection is premised on a mistaken understanding of the art. As such, *prima facie* obviousness has not been established.

Moreover, the Action again asserts that, because an ID card may be used for government use, it would have been obvious that the central network can be a government agency.

Again, that's hindsight. Although government agencies have maintained image archives for years, Appellants' specification is believed to be the first to teach or suggest that an individual may obtain their own archived photo *from* a government agency.

The rejection is multiply flawed and should be reversed.

**18. Claim 12 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 12 stands or falls with the Rhoads-based rejection of claim 11.

**19. Claim 13 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 13 stands or falls with the Rhoads-based rejection of claim 11.

**20. Claim 14 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 14 stands or falls with the Rhoads-based rejection of claim 13.

**21. Claim 15 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 15 stands or falls with the Rhoads-based rejection of claim 14.

**22. Claim 21 (§ 103 Rhoads)**

Claim 21 is an independent claim that reads as follows:

*21. A method of providing an access credential for a person, using a computer device for which the person is the proprietor, the method comprising:  
receiving at said computer device code data, transmitted by an authority, the code data having a future time or date associated therewith;  
steganographically encoding said code data in a graphic; and  
presenting the encoded graphic as an access credential, to gain access to a restricted area.*

The Office wrongly asserts that Rhoads teaches the first limitation, citing col. 1, lines 27-34, and noting that driver's licenses have expiration dates.<sup>25</sup> The cited passage states:

*The use of photograph-based identification ("photo ID") systems is pervasive. Drivers' licenses, passports, visas, government employee cards, immigration documents, and now, more frequently, credit cards and cash transaction cards carry a photograph of the card bearer for identification purposes. Many industries require that their employees carry photo ID on the job.*

This passage does not teach "receiving at said computer device code data, transmitted by an authority, the code data having a future time or date associated therewith."

Moreover, while a driver's license has an expiration date, this is not code data transmitted by an authority and received at a person's computer device.

Again, the rejection is based on a mistake of fact. As such, *prima facie* obviousness has not been established. Reversal is again required.

**23. Claim 22 (§ 103 Rhoads)**

Claim 22 depends from claim 21 and is similarly allowable. Moreover, claim 22 is patentable independently. The claim reads:

---

<sup>25</sup> Final Action, page 7, last 3 lines.

*22. The method of claim 21 that includes steganographically encoding said code data in said graphic using said computer device.*

The “said computer device” that steganographically encodes the graphic, is the *person’s* computer (as contrasted with the authority’s computer).

The Final Rejection wrongly asserts that Rhoads’ Fig. 3, and 29 lines in col. 3, teach this limitation.<sup>26</sup> However, they do not.

Again, the rejection is based on a mistake of fact. Reversal is again required.

**24. Claim 23 (§ 103 Rhoads)**

Claim 23 depends from claim 21 and is similarly allowable. Moreover, claim 23 is patentable independently. The claim reads:

*23. The method of claim 21 that includes printing said encoded graphic using a printer for which said person is also the proprietor, and presenting the printed graphic as said access credential.*

Despite the fact that none of the cited art teaches a person printing their own access credential using their own printer, the Final Rejection contends same is obvious.

Again, prior to Appellants’ work, self-printing of access credentials has been subject to obvious security flaws. An artisan would tend to *avoid* such procedures. There is no suggestion of self-printed access credentials in the cited art. The Office’s conclusion appears impermissibly motivated by hindsight.

Again, reversal is required.

**25. Claim 24 (§ 103 Rhoads)**

Claim 24 depends from claim 21 and is similarly allowable. Moreover, claim 24 is patentable independently. The claim reads:

---

<sup>26</sup> Final Action, page 8, lines 15-17.

*24. The method of claim 21 in which the access credential authorizes entry to an event, the event taking place at said future time or date.*

This claim is dismissed by the practice of movie theatres to require display of a driver's license prior to admitting a patron to an 'R' rated movie.

The cited practice does not suggest the limitation of claim 24, in the context defined by claim 21. Again, reversal is required.

**26. Claim 25 (§ 103 Rhoads)**

The Rhoads-based rejection of claim 25 stands or falls with the Rhoads-based rejection of claim 24.

**27. Claim 26 (§ 103 Rhoads)**

Claim 26 depends from claim 21 and is similarly allowable. Moreover, claim 26 is patentable independently. The claim reads:

*26. The method of claim 21 that includes receiving said graphic from a governmental agency.*

The Final Rejection dismissed this claim with the same wording that was offered against claim 23. However, the claims present different limitations.

None of the art suggests receiving a graphic from a governmental agency, and code data from an authority, and steganographically encoding the latter into the former to provide an access credential – using a computer device for which the person is the proprietor.

Again, *prima facie* obviousness has not been established, and the rejection should be reversed.

**VIII. CONCLUSION**

None of the rejections meets the Office's burdens. Accordingly, the Board is requested to reverse the pending rejections and remand for issuance of a Notice of Allowance.

Date: November 3, 2005

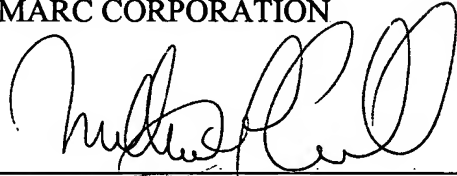
**CUSTOMER NUMBER 23735**

Phone: 503-469-4800  
FAX 503-469-4777

Respectfully submitted,

DIGIMARC CORPORATION

By

A handwritten signature in black ink, appearing to read 'William Y. Cornwell', is written over a horizontal line.

William Y. Cornwell  
Registration No. 31,943

**APPENDIX A**  
**PENDING CLAIMS**

1. A method of printing a trusted image, comprising:  
an individual user electronically contacting a governmental agency, soliciting an image depicting the user stored in an archive maintained by said governmental agency;  
electronically receiving said image from said contacted governmental agency; and  
printing a document incorporating said image.
2. The method of claim 1 in which it is the individual user who receives said image and prints said document.
3. The method of claim 1 in which said document is a photo identification document.
4. The method of claim 1 in which said document is an identification badge.
5. The method of claim 1 in which the governmental agency is a motor vehicle licensing agency, and the image is a driver license photo.
6. The method of claim 1 in which said image is processed with an identification code by the governmental agency.
7. The method of claim 1 in which said image is digitally watermarked with a plural-bit code by the governmental agency.
8. The method of claim 7 in which said plural-bit code serves to identify the individual user's name.
9. The method of claim 8 in which said plural-bit code comprises an index into a data

structure in which the individual user's name is stored.

10. A document printed according to the method of 1.

11. A method of distributing a trusted image, comprising:  
at a governmental agency, receiving an electronic request for an archived personal image from an individual depicted in said image; and  
electronically transmitting said image to said individual.

12. The method of claim 11 that includes processing said image with an identification code prior to said electronic transmission.

13. The method of claim 11 that includes digitally watermarking said image with a plural-bit code prior to said electronic transmission.

14. The method of claim 13 in which said plural-bit code serves to identify the individual's name.

15. The method of claim 14 in which said plural-bit code comprises an index into a data structure in which the individual's name is stored.

16. A document printing method, comprising:  
receiving a digital photo, the photo having plural-bit data steganographically encoded therein;  
by reference to said steganographically encoded data, generating text to be printed with said photo; and  
printing a document including both said photo and said text.

17. The method of claim 16 that includes electronically transmitting at least a part of said plural-bit data to a remote computer, and receiving the text from said computer.

18. The method of claim 16, that includes receiving said digital photo from an archive of facial images.

19. The method of claim 16 that includes receiving said digital photo from an image archive maintained by a government agency.

20. The method of claim 16 in which said document is an identification document.

21. A method of providing an access credential for a person, using a computer device for which the person is the proprietor, the method comprising:

receiving at said computer device code data, transmitted by an authority, the code data having a future time or date associated therewith;

steganographically encoding said code data in a graphic; and

presenting the encoded graphic as an access credential, to gain access to a restricted area.

22. The method of claim 22 that includes steganographically encoding said code data in said graphic using said computer device.

23. The method of claim 21 that includes printing said encoded graphic using a printer for which said person is also the proprietor, and presenting the printed graphic as said access credential.

24. The method of claim 21 in which the access credential authorizes entry to an event, the event taking place at said future time or date.



25. The method of claim 24 wherein the event is a movie.
26. The method of claim 21 that includes receiving said graphic from a governmental agency.